11 FISCAL/EQUIPMENT MANAGEMENT *Effective: 3/1/97*
11.7 Appropriate Use of WIC Computers *Revision: 7/1/01*

POLICY: Computers and telecommunication resources purchased with WIC funds may be used for business purposes only. See also Policy 11.8 Putting DAISy on an Agency Lan and 11.10 E-Mail and Internet Access for Local WIC Staff.

BACKGROUND: Public Law 98-473, The Computer Fraud and Abuse Act of 1986, revised by Public Law 98-474, provides for punishment of individuals who access Federal computer resources without authorization; attempt to exceed access privileges; abuse Government resources; and/or conduct fraud on Government computers. Since most computers used within local WIC projects were purchased with state and/or federal funds, the same guidelines will apply.

Employees may use e-mail as a communications tool, understanding that an e-mail message is considered a "public record" and therefore is subject to the provisions in Wis. Stats. Chapter 19, Subchapter II, Public Records and Property, Sec. 19.21-.39.

PROCEDURE:

A. WIC STAFF RESPONSIBILITIES
WIC employees share the responsibility for ensuring that WIC computers are used only for business related activities. The following activities describe the conduct necessary to meet this expectation.

1. Ensure that only authorized and licensed software is loaded on WIC computers the employees use.

2. Use WIC information systems resources only for authorized purposes.

3. Do not use WIC computers or software for unauthorized monetary gain or illegal activity.

4. Adhere to all security procedures and policies to ensure safety and confidentiality of WIC data.

5. Do not modify WIC computer equipment and software for personal use.

6. Do not use WIC information systems resources to store information that is not related to WIC business.

B. WIC PROJECT DIRECTOR RESPONSIBILITIES

1. Ensure that the employee is using WIC computers and software for authorized purposes only.

2. Ensure that the employee does not use computer hardware or software for personal monetary gain.

3. Ensure that all applicable security procedures and policies are followed.

4. Ensure that the employee does not load unauthorized software on WIC computers or any software on LAN attached computers.

C. LOCAL LAN ADMINISTRATOR RESPONSIBILITIES

1. Periodically check to make sure that only WIC or supervisor approved software is loaded on LAN attached or stand-alone computers.

2. In the event that unauthorized and/or unlicensed software is detected, the local LAN Administrator should remove the software in question from the computer and notify the employee's supervisor.

3. Deinstall or delete any games that come with a software package.